DEPARTMENT OF COMPUTER SCIENCE

Trustworthy Artificial Intelligence and Internet of Things

- Adversarial machine learning and generalization
- Secure and privacy-preserving federated learning
- Explainable and robust AI for medicine and healthcare •
- Time series analysis and anomaly detection for IoT & edge computing

CEC Research



